Volume 7, Issue 16   Atari Online News, Etc.   April 15, 2005

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Kevin Savetz

=~=~=~=

A-ONE #0716   04/15/05

~ Florida Beats Spammers ~ People Are Talking!   ~ Mac OS Tiger Soon!

```
     ~ Bush Averse to E-mail! ~ Firefox Still Drawing! ~ New ID Theft Focus!
     ~ Murdoch Urges Web News ~ Pols Tackle Spyware!   ~ Studio Son Is Back!
     ~ Seagate New Technology ~ Xbox To Debut On MTV!  ~ Containing Spam!

                    -*  Microsoft To Pay Gateway!   *-
                   -* Colleges Form Cyber Security Group! *-
                  -* Internet Users Are More Accepting of Spam? *-



                              =~=~=~=



->From the Editor's Keyboard              "Saying it like it is!"
  """"""""""""""""""""""""""
```

Did I say something wrong last week? If I remember correctly, I was
complimenting the weather. So, what's with the blast of snow a few days
ago? One last reminder? It was a terrific weekend; I managed to get most
of the yard cleaned up of some remnants of the fall and winter. Plants are
breaking through the ground. What a terrific time of year!

Let's get on with this week's issue. I don't have a lot on my mind at the
moment (what a surprise!), and I'm feeling more attuned to enjoying the
weather than writing at the moment.

Until next time...


```
                              =~=~=~=



                    Studio Son Sound Sample Editor
```

DOCs has announced:

After several years of absence, Studio Son, the sound samples editor for
Falcon, is back with the 2.08 beta release (up to date, only in French).
The main improvement is the new function "Filtering..." which enables you
to produce FIR filters (Low Pass, High Pass, Band Pass and Band Reject).
This is carried out by the DSP 56001 and with Direct to disk process.

I must still work to add errors managements and other features, so
please wait...

This is a beta version, so be careful with your samples, do not totally
trust in this program. You must know I have not noticed any problems.

You can find 68030 and 68030+68882 versions in the archive.

http://doyeuxyvan.free.fr/stud>ioson/std208b/STD208B.ZIP

```
                              =~=~=~=



                         PEOPLE ARE TALKING
                       compiled by Joe Mirando
                         joe@atarinews.org






                              =~=~=~=




->In This Week's Gaming Section  - New Xbox To Debut On MTV!
  """"""""""""""""""""""""""""""""    Crash Tag Team Racing!
                                      UN Game: Feed, Not Kill!






                              =~=~=~=




->A-ONE's Game Console Industry News   -  The Latest Gaming News!
  """""""""""""""""""""""""""""""""""""""



               Microsoft to Unveil Next Xbox on MTV May 12


Microsoft Corp. on Monday said it would unveil the next generation of its
Xbox video game console in a May 12 special on music and entertainment
cable channel MTV.

The unveiling will be a first, as video game companies usually take the
wraps off their new consoles at exclusive industry events like the trade
show E3 - which will be held the following week in Los Angeles.

"I think we need to signal a change that things aren't going to be the same
in the next generation," said Peter Moore, corporate vice president in the
Xbox division, in an interview. "While it's gaming at its core, there's a
much bigger and broader entertainment message that we need to get out
there."

Microsoft said the special would also air in Japan the morning of May 13
and across Europe that evening.

The special will include footage of next-generation Xbox games and also
online play, Microsoft said. Actor Elijah Wood will host the show, with
local hosts for each country.

The company has not set a release date for the Xbox successor or even
announced a name, but the new hardware is expected to be released later
this year.
```

Market leader Sony Corp. has said little about the timetable for its next-generation PlayStation console, but there is speculation it will offer details at E3 next month.

Last week Sony advised it would hold its E3 press conference a few hours before Microsoft's, a break with tradition that some saw as a sign Sony wanted to steal Microsoft's anticipated thunder.

Moore said Microsoft has been planning the MTV launch since last year and only found out about the Sony schedule change last week.

Moore said the show will be "live to tape," meaning it will be filmed as though it were a live event, and edited later to add celebrity interviews and the like.

Crash Tag Team Racing In Development For Consoles

Vivendi Universal Games (VU Games) announced the development of Crash Tag Team Racing for the PlayStation 2 computer entertainment system, the Xbox video game system from Microsoft, Nintendo GameCube and Nintendo DS. Developed by Radical Entertainment, creators of the critically-acclaimed The Simpsons: Hit & Run, and Sensory Sweep (Nintendo DS version), the newest addition to the best-selling video game franchise will give players a unique racing experience and allow them to continue the adventure on foot with out-of-car action. For the first time ever in a racing game, players will be able to fuse two cars together on the fly to form a super vehicle with the all-new 'clashing' technology.

In Crash Tag Team Racing, players can combine their car with an opponent's mid-race to make a super-car equipped with a powerful turret gun. When clashed, players can either get behind the wheel and drive or fire an onboard weapon. Each character has his or her own uniquely deadly 360 rotating turret. Players can continue the action out of the car where they can explore the entire world on foot and collect upgrades for their cars and unlock bonus tracks.

Crash Tag Team Racing features split-screen multiplayer for up to eight players with system link on all consoles, and wirelessly supports up to four on the Nintendo DS.

"We"re thrilled to give Crash Bandicoot fans another hilarious adventure with the irrepressible marsupial," said Ian Wilkinson, President, Radical Entertainment. "The development team showed off its ability to create a break-out vehicle-based game with The Simpsons: Hit & Run and is set to deliver another innovative and wildly fun title in Crash Tag Team Racing."

Penned by Crash Twinsanity writer Jordan Reicheck, best known for his work on Ren & Stimpy, Crash Tag Team Racing brings the trademark Crash Bandicoot humor to new levels. After being humiliated yet again by Crash Bandicoot at the end of Twinsanity, Dr. Neo Cortex returns to his evil scheming in his dilapidated Iceberg Lair. He hatches a sinister plan to challenge Crash to a seemingly friendly race competition, with plans of crushing the hapless bandicoot under the ruins of the hazardous racetrack!

Crash Tag Team Racing will be available at retail in Fall 2005 for a suggested retail price of $39.99 (Xbox, PlayStation 2 and Nintendo

GameCube) and $29.99 (Nintendo DS).

                    U.N. Video Game Encourages Kids to Feed, Not Kill

The jungle territory that hides lurking rebel forces makes it look like a
shoot-em-up adventure, but in this video game - from the U.N.'s food aid
agency - the aim is to feed the masses rather than blow them away.

The U.N. World Food Programme (WFP) hopes the game "Food Force," in which
players direct aid workers trying to help the poor, will teach children
about the problems of feeding the hungry, especially those trapped in war
zones.

"So many parents complain about the blood and gratuitous violence that kids
are so frequently exposed to in video games. This is a fun action-packed
alternative," said WFP spokesman Neil Gallagher, launching the game on
Thursday.

The game challenges players to get food into the fictional war-torn island
of Sehylan - finding the hungry people, dropping aid from a helicopter,
dealing with hostile forces and setting up "Sim City" style farm projects
for the future.

"Communicating with children today means using the latest technology," said
Gallagher. "Food Force will generate kid's interest and understanding about
hunger, which kills more people than AIDS, malaria and tuberculosis
combined."

The PC-based game can be downloaded for free from the Web Site
www.food-force.com. A separate section called "How to help" tells children
how to get involved in fundraising and community work.

                              =~=~=~=

                         A-ONE's Headline News
                   The Latest in Computer Technology News
                      Compiled by: Dana P. Jacobson

                     Microsoft to Pay Gateway to End Dispute

Microsoft Corp. will pay computer maker Gateway Inc. $150 million over four
years to end a long-running legal dispute, and Gateway says it will use the
money to market and develop products that run Microsoft software.

As part of the settlement announced Monday, Gateway will release all
antitrust claims against Microsoft based on past conduct. Microsoft denies
any wrongdoing.

To account for the settlement, Redmond-based Microsoft said it would take
a $123 million pretax charge in the quarter ended March 31. The company

also plans to take a pretax charge of $41 million for an earlier settlement with Burst.com. And it will take an additional $550 million charge to reserve funds for other antitrust matters, such as its ongoing legal wrangling with digital media rival RealNetworks Inc.

The deal marks the latest in a series of agreements Microsoft has reached to put various antitrust claims behind it.

"Obviously Microsoft wants to get as many legal barriers out of the way as possible," said Alan Davis, an analyst with Seattle-based McAdams Wright Ragen.

Davis said the Gateway settlement was "below the radar" compared with what Microsoft has done with bigger cases, and he noted the software company has billions of dollars in cash reserves.

"It's definitely not going to make a big dent in Microsoft's cash balance," he said.

Over the past two years, Microsoft has spent some $3 billion to settle private antitrust lawsuits filed by Time Warner Inc., Sun Microsystems Inc., Be Inc. and Novell Inc. It also paid an undisclosed amount to a trade group that had backed antitrust complaints by the U.S. government and the European Union.

Microsoft still faces some antitrust hurdles.

The Novell settlement relates to antitrust claims regarding its NetWare product. Less than a week after reaching that deal, Novell filed a lawsuit regarding WordPerfect, a product Novell used to own.

Microsoft also has been sued by Seattle-based RealNetworks, and is currently appealing a more than $600 million European Union antitrust ruling against it.

In a statement, Irvine, Calif.-based Gateway said it would use its settlement money for creating new personal computer products that work with current and future Microsoft software, including the planned new Windows operating system.

"Gateway continues to enjoy a strong relationship with Microsoft and we're pleased to put these legacy legal issues behind us," said Wayne Inouye, president and chief executive of Gateway.

The Gateway antitrust claims arose from Microsoft's long-running U.S. government antitrust case. At one point during that case, U.S. District Judge Thomas Penfield Jackson specifically identified Gateway as a company that had been hurt by Microsoft's business practices.

Microsoft later reached a landmark antitrust settlement in that case, which was approved by a federal court in October 2002.

Under the statute of limitations, Gateway had until late 2003 to bring a case against Microsoft based on the federal case's finding. But the companies said in a statement Monday that they had agreed to extend that period while they brokered a deal.

The companies said Monday's agreement resulted from a recent mediation but would not give any more specific timing.

Universities Form Cyber Security Group

A consortium of colleges will lead an effort to bolster the nation's cyber security, forming a center funded by the National Science Foundation.

Helmed by the University of California, Berkeley, the cybersecurity center will investigate issues surrounding computer trustworthiness, and will operate under the name Team for Research in Ubiquitous Secure Technology (TRUST).

The center is expected to receive approximately US$19 million over the next five years, and could be given a 5-year extension after that point.

Although it will concentrate on research, the center could also yield some new technologies that are worthy of development.

The NSF notes that the center will lead development of these technologies based on findings from studies of software and network security, trusted platforms and cryptographic protocols.

The TRUST center also will examine the types of security problems that plague systems, and to what effect trusted components and security information management software can make systems more secure.

Beyond merely examining hardware and software, the center also will look at how cybersecurity impacts society and affects economic conditions.

"This is a broad program because computers have a tremendous impact on our lives, and on science," said NSF spokesperson William Noxon.

"We believe it's important because these issues cut across society," he added. "This isn't just an I.T. issue."

The NSF has been especially struck by all the reports of malicious hackers worming their way into allegedly protected systems, Noxon said.

With so much scientific and economic research depending on computers, the TRUST center is a preemptive strike against future threats.

"We have to stay ahead of security problems, we have to figure out how to stop them before they begin," he noted. "That's what this center will be trying to determine through the next five years."

Colleges teaming up with Berkeley for the TRUST center include Carnegie Mellon University, Cornell University, Mills College, San Jose State University, Smith College, Stanford University and Vanderbilt University.

Several major companies have also signed up to help the project, including Microsoft, Hewlett-Packard, IBM, Sun Microsystems and Symantec.

The center plans to have an education outreach component to K-12 schools, undergraduate students and institutions serving underrepresented populations, according to the NSF. The goal is to develop the next generation of scientists and engineers who can continue the work of building trustworthy systems.

Congress Moving to Tackle Spyware Problem

An anti-spyware bill could clear the U.S. House of Representatives as early as next week, but final legislation is not expected to be sent to the White House until disagreements about what qualifies as "spyware" are ironed out by key technology interest groups and lawmakers.

Spyware is a catchall term used to describe programs that stealthily install themselves on computers. Some versions - often referred to as "adware" - spawn numerous pop-up advertisements when computer users attempt to navigate the Internet. Other, more intrusive versions can track online movements, steal passwords and sensitive data, and give hackers control over infected computers.

Even the least-intrusive spyware programs can severely restrict an infected computer's ability to carry out basic functions like surfing the Web and word processing.

Experts say the spyware problem has grown to near epidemic levels, rivaling the problem with e-mail spam. Last October, America Online and the National Cyber Security Alliance examined the computers of 329 randomly selected Internet users and found that 85 percent of them contained some form of spyware. The average "infected" computer had more than 90 spyware and adware programs.

The research firm IDC estimated last year that people would spend $305 million a year on anti-spyware software in 2008, up from $12 million in 2003.

Three separate proposals have been introduced in Congress so far this year - two in the House and one in the Senate. A bill sponsored by Rep. Mary Bono (R-Calif.) appears to have the most momentum, earning the backing of Rep. Joe Barton (R-Texas), chairman of the influential Energy and Commerce Committee.

"The consumer should have the right to know what's going on with their computer. It's their property and they should know what's happening. The bottom line is that people cannot install something on your computer and track you and eat up all the processing power on your computer without your consent," Bono said.

Internet service providers whose customers are most at risk to the spyware threat are urging quick action.

"Spyware is obviously a problem that affects virtually all Internet users. While the [Bono] bill will not be a cure-all, we support congressional attempts to counteract this problem. As was the case with spam we have to fight the problem on several fronts using legislation litigation enforcement, customer education and technology solutions," said Dave Baker, vice president of law and public policy for Atlanta-based Earthlink.

Lawmakers and lobbyists with a stake in the spyware debate agree that Congress is likely to pass a federal law sometime this year, though what that final language will look like remains up in the air.

Each of the three spyware bills targets the nastiest practices associated with spyware, some of which are already illegal. But they differ both in the penalties they create and in how they define spyware.

It's those definitions that have some in the high-tech industry nervous.
They fear that a bill designed to stamp out spyware could inadvertently
put legitimate software - such as the kind used to automatically update
anti-virus and other software programs - on shaky legal ground.

"One of the profound difficulties that we keep facing as we're talking
about this is that there is a massive disconnect between what spyware
really is and what is considered to be spyware," said Robert Cresanti, the
vice president for public policy at the Business Software Alliance, which
represents companies like Microsoft, Symantec and Cisco Systems.

"A likely scenario could put legitimate companies at high risk for what
might be a technical violation of the bill without any ill intent,"
Cresanti said. The BSA agrees that anti-spyware legislation is needed, but
the group wants to make sure that the final bill doesn't hurt legitimate
businesses, he said.

Bono's Spy Act, which cleared the Energy and Commerce Committee by a
unanimous vote March 9, would require companies to obtain permission
before they install any program that collects information on a person's
computer.

"We're much more concerned about that section of the bill. We don't think
it's responding to an immediate need in the market, and we think it has
the potential for some pretty serious collateral damage against an industry
that is really burgeoning right now," said Trevor Hughes, executive
director of the Network Advertising Initiative, which represents online
advertising companies like DoubleClick and 24/7 Real Media.

Hughes said there are dozens of advertising-supported Web site features -
like stock tickers and personalized weather reports - that could be
affected under those definitions.

Although Bono's bill does not restrict the use of "cookies" - the small
tracking programs used by Web sites to maintain things like virtual
shopping carts and other visitor-specific content - Hughes said it could
drag in many common programs used by Web operators to personalize the
online experience.

"Web sites are very sophisticated commercial operations nowadays, and there
may be 15 commercial entities operating on the same site," Hughes said. "If
the consumer has to click through 15 different boxes saying yes I want
this, no I don't want this, that's really going to impede the online
experience."

Bono said the current version of her bill, which has gone through several
drafts, addresses the concerns raised by the high-tech industry, but still
provides protection to consumers. "We've tried to accommodate industry
along the way. It's come a long way but [we've] been trying to walk that
fine line between keeping the industry people happy and the privacy people
happy. "

In the Senate, Conrad Burns's (R-Mont.) Spy Block Act also targets a class
of computer programs that collect information without computer users'
knowledge. It was this aspect of the bill that concerned Sen. George Allen
(news, bio, voting record) (R-Va.) last year when it appeared that Burns's
bill was headed for passage.

"If you define a specific illegal spyware activity it is very difficult to

do so without causing legitimate software companies unintended consequences and unneeded burdens," Allen said.

Allen said he was also concerned that the law could inadvertently create a "safe harbor" for some malicious spyware distributors - allowing them to hide behind consent language that users may agree to without fully reading.

Both Hughes and Cresanti said their organizations would prefer that an anti-spyware bill target the behavior of spyware distributors, rather than a whole class of technology that has legitimate uses.

Allen said he plans to introduce legislation as early as next week in the Senate that would stiffen existing anti-fraud penalties for anyone convicted of committing fraud via spyware. Allen's bill would also authorize about $10 million for law enforcers to go after spyware distributors. "Much, if not everything, they are trying to create a new definition of a crime for is already against the law," Allen said.

That's also been the primary argument of the Federal Trade Commission. "Most of the acts and practices and harm consumers that are covered under these bills are things that would be either unfair or deceptive under the FTC Act," said Tom Pahl, an assistant director in the FTC's Division of Advertising Practices. Under each of the congressional proposals, the commission would be saddled with coordinating federal enforcement efforts.

According to Bono, the regulators aren't doing enough. "I believe the FTC has been asleep at the wheel so far and hasn't enforced it and that's why it's grown so exponentially," she said, adding that her bill would give Congress the ability to "hold the enforcers' feet to the fire."

The FTC has brought a handful of spyware cases, Pahl said, but the agency has been hindered by the fact that many spyware distributors are located overseas. The commission has asked Congress to pass legislation that would make it easier for them to coordinate with foreign law enforcers.

Pahl added that Congress already pressures the commission to bolster its enforcement efforts. "Congress can and does hold our feet to the fire for how we enforce the FTC Act. Chairman Barton is very adept at holding our feet to the fire and he doesn't need a new law for that," he said.

                    Florida Wins First Injunction Against Spammers

The U.S. state of Florida won its first victory against "spam" electronic mail when a judge granted an injunction against two men accused of running mass emailing operations, the state prosecutor said on Tuesday.

Florida Attorney General Charlie Crist said the injunction preventing the men from sending any more deceptive emails was part of his department's first prosecution under an anti-spam law passed by the state legislature last year.

The men, Scott Filary, 25, and Donald Townsend, 34, both of Tampa, are accused of sending more than 65,000 emails, many with misleading subject lines and disguised origins.

The emails took recipients to Web sites Crist said were engaged in fraudulent or illegal activities, such as selling pharmaceuticals and

cigarettes online or providing a platform for the illegal downloading of copyrighted movies.

The investigation was aided by software giant Microsoft Corp., whose Windows operating system runs more than 90 percent of the world's computers.

The Florida anti-spam law allows for a fine of up to $500 per email, or $24 million in the case of the two accused spammers, Crist said in a statement.

A national anti-spam law took effect at the start of 2004 but has done little to curb the flood of spam clogging email inboxes.

Spam is estimated to account for more than 80 percent of all email traffic, costing businesses billions a year in lost productivity and bandwidth.

A court in Virginia jailed a North Carolina man this week to nine years in prison for sending millions of pieces of spam, although the judge postponed the sentence while the case was appealed. It was the nation's first felony prosecution of a spammer.

                    Internet Users More Accepting of Spam

We're not any less annoyed by spam. We're just more accepting of it. So says a study released Sunday by the Pew Internet and American Life Project.

Fifty-three percent of adult e-mail users in the United States now say they trust e-mail less because of spam, down from 62 percent a year ago and about the same as a June 2003 Pew survey.

Pew also found that 22 percent of e-mail users say they are spending less time on e-mail because of spam, down from 29 percent last year. In 2003, it was 25 percent.

"This shows some level of tolerance that people are manifesting," said Deborah Fallows, a senior research fellow at Pew and the study's author. "Maybe it's their getting used to it. Maybe it's like other annoying things in life - air pollution, traffic - they are just learning to live with it."

Pornographic spam is on the decline, replaced by fraudulent "phishing" scams aimed at stealing bank passwords and other sensitive information, the study finds.

There was little change in what people do to reduce spam.

About the same percentage avoid giving out e-mail addresses or set up special addresses when they believe they might attract spam. In fact, a lower percentage avoid posting e-mail addresses on Web sites, where spammers often collect addresses for their mailings.

However, there was a slight increase in the percentage of e-mail users who set up hard-to-guess addresses - such as "joe342d3x" - to make it more difficult for dictionary attacks, in which spammers try to send junk to any address they could think of by trying various combinations of words found in the dictionary.

The telephone-based survey of 1,421 Internet users was conducted Jan. 13 to

Feb. 9 and has a margin of sampling error of plus or minus 3 percentage
points.

                    Battle Against Spam Shifts to Containment

There's a new strategy in the spam battle: Call it containment.

Filters for blocking junk e-mail from inboxes have improved to the point
that doing much more will needlessly kill legitimate e-mail, said Carl
Hutzler, America Online Inc.'s anti-spam coordinator. So e-mail gatekeepers
are shifting gears.

Now they're getting more aggressive at keeping spam from leaving their
systems in the first place.

EarthLink Inc., for instance, is phasing in a requirement that customers'
mail programs submit passwords before it will send out their e-mail.

Like most Internet providers, EarthLink previously made sure only that a
computer was associated with a legitimate account. Now that viruses can
co-opt computers and use them to send spam, that's no longer secure enough.

So Earthlink sent out new software, made automated tools available for
download and walked customers through manually changing their mail settings
when they called tech support for other reasons. A year into the
initiative, EarthLink has 80 percent of its customers converted.

"Any action can be a little daunting when you're trying to migrate millions
of people," said Stephen Currie, EarthLink's director of communications
products.

It also costs time and money - not insignificant considering that direct
benefits don't necessarily go to EarthLink but to its competitors, whose
customers might otherwise receive more spam.

But more than altruism was involved.

"If there's a lot of spam or abusive mail coming from a particular network,
in the future you're going to see that e-mail having low rates of
deliverability," Currie said.

In other words, other Internet service providers, or ISPs, might start
blocking EarthLink e-mail if it doesn't adopt the outbound controls.

The pressure to improve outbound controls comes as viruses infect more and
more home computers and convert them into spam-relayng "zombies."

These zombies allow spammers to pose as legitimate customers and get around
blocks that Internet providers might have had in place.

Although antispam advocates say Internet providers can do more to stop
spammers from signing up for accounts - sometimes fraudulently, but too
often because they mean revenues and sales commissions - Hutzler blames
zombies for 90 percent of the spam problem.

Traditional spam controls, the inbound filters, don't work as well with
zombies because they can block mail from legitimate customers, too.

Outbound controls can target specific zombies.

"The best place to stop spam is before it's sent," said John Reid, a volunteer with The Spamhaus Project anti-spam group. "If you can keep it in the bag, bottled up, that's where it's the least expensive."

Outbound controls aren't entirely new.

For years, anti-spam advocates have been pressuring Internet providers to configure mail servers so spammers can't use them to relay junk e-mail. The leading vendor of mail server software, Sendmail Inc., closed such relays by default in 1998, and most ISPs now have the newer software.

EarthLink and AOL also have long implemented a technique that forces customers to route e-mail through the providers' own mail servers, instead of sending messages directly to the Internet.

Other ISPs are starting to adopt it as well, giving them the ability to monitor outgoing mail, trace any problems to specific accounts and even block or place speed limits on e-mail that exceeds some hourly or daily threshold.

ISPs can also run the spam and virus filters on outbound mail.

And when users of Microsoft Corp.'s Hotmail try to send a large number of messages, they are prompted to type in random letters displayed on the screen. Presumably, spammers with automated tools wouldn't be able to do it.

If all ISPs were to implement outbound controls, spam wouldn't be such a headache.

But outbound measures are often difficult to justify because they don't directly pare down the junk in customers' inboxes as inbound filters do, said Anne Mitchell, who runs the Institute for Spam and Internet Public Policy, an antispam consultancy.

Mitchell said ISPs are businesses and "have to look at the bottom line and their profitability."

Besides implementation costs, outbound measures can hurt legitimate customers.

Businesses and some individuals might have a legitimate need to access third-party mail servers, and being forced to go through their providers' systems might cause their e-mail to be mistakenly tagged as spam by the recipient.

Anytime ISPs make changes, they will invariably discover a few customers who use their service in an unanticipated, but legitimate manner, said John Levine, co-author of "Fighting Spam for Dummies."

Martin Deen, manager of messaging engineering at Cox Communications Inc., likens outbound measures to vaccination. They may be good for the overall health of the Internet if all ISPs do it, Deen said, but individual ISPs take a personal risk.

ISPs sometimes grant exceptions for businesses and power users.

AOL has a few thousand customers, out of more than 28 million, who are

exempt from caps on multiple mails.

Desert Express Internet Services, a small ISP serving California and Nevada, waived its restrictions for one of its business customers - but only if it agreed in writing to run spam filters on outgoing mail and meet other requirements.

Ultimately, ISPs may require customers with special needs to buy a premium service.

"We don't do that, (but) that would be a possibility certainly," EarthLink's Currie said. "EarthLink and other ISPs are just going to define their services, and certain things will be permitted and certain won't."

Congress Renews Interest in Identity Theft

Responding to outrage from consumers whose personal information has been stolen from companies, Congress is primed to pass new laws to try to prevent break-ins and to require businesses to confess to customers when private data is taken.

The government's new interest in requiring such embarrassing disclosures reverses years of efforts by the FBI and U.S. prosecutors to shield corporations that have been victims of hackers from bad publicity by keeping such crimes out of headlines.

But now, consumers want to know if their private information has been stolen.

The Senate is considering at least two proposals to crack down on companies suffering breaches of private customer information. The Federal Trade Commission's chairwoman has endorsed the idea and the Senate Judiciary Committee's chairman hinted this week that a new law might be inevitable.

"We may well face a necessity for some really tough legislation," said Sen. Arlen Specter (news, bio, voting record), R-Pa.

The new push for government action responds to frustrated constituents who are among more than 10 million victims of identity theft each year. It comes after years of reluctance by most companies to voluntarily report break-ins that put customers' financial information at risk.

"Congress is primed to take a very serious look at this and pass comprehensive legislation," said Sen. Charles Schumer (news, bio, voting record), D-N.Y., sponsor for one bill. "Nobody has given this problem the focus it deserves. This is a high priority."

A California law already requires disclosures to victimized consumers who live there, and roughly 30 states are looking at similar laws.

"The last thing a merchant wants to do is tell all his longtime customers he's been hacked and lost all their information," said Keath Nupuf, chief technology officer for CardCops Inc. of Malibu, Calif. The company monitors Internet chat rooms and other hacker communications for stolen credit card numbers, then notifies merchants and consumers to block bad purchases.

CardCops contacted 80 consumers earlier this week to report their card

numbers and other personal details were circulating among Internet thieves, Nupuf said. The card numbers were pilfered from merchants that range from mom-and-pop shops to Fifth Avenue retailers.

"One guy was blowing a blood vessel," he said. "He was going to drive across country and kill the merchant."

Peiter "Mudge" Zatko, a computer expert who consulted for the White House during the Bush and Clinton administrations, often is hired by companies to tighten security and clean up the digital mess after a data breach. Zatko said victim companies "almost never" tell the FBI or customers when sensitive data is stolen.

"Maybe they have a government contract and it would look bad," Zatko said. "Maybe they're trying to keep it quiet so they don't scare the financial markets."

Sometimes companies warn customers. Howard Schmidt, a former White House adviser, said thieves took a computer this year from the store where he buys eyeglasses. The computer contained his credit and medical information, Schmidt said, but the owner contacted his customers and encouraged them to watch for fraudulent purchases.

"That was a good thing," Schmidt said. "I want to do business with these guys."

In a twist, the FBI and Justice Department have worked aggressively to shield the identities of corporations that have been hacking victims. To encourage businesses to contact them after such break-ins, U.S. investigators and prosecutors have publicly promised to seal court records, keep top executives off witness stands and use protective orders to keep details of these crimes out of the headlines.

"There is still some reluctance to call law enforcement, some hesitancy because of the negative impact on reputation," said Amit Yoran, the Bush administration's former top cyber-security official. He said requiring companies to acknowledge a break-in "may be of value, but it should not be done as a knee-jerk reaction to the handful of high-profile and significant disclosures of the past few weeks."

The FTC chairwoman, Deborah Majoras, estimated consumers lost $5 billion and businesses lost $48 billion because of identity theft in 2003. The FTC is studying how it can use existing banking statutes and laws against consumer fraud to prosecute companies that fail to report serious breaches.

Majoras said government should consider requiring companies to tell customers about break-ins when thefts put them at financial risk. She also endorsed minimum security requirements for businesses that collect sensitive personal information.

"The challenge is to come up with a way of defining when notice should be sent and when it doesn't make sense," said Joel Winston, associate director at the FTC's division for financial practices.

Apple to Ship Mac OS X Tiger Software on April 29

Apple Computer Inc. said on Tuesday that the latest major update of its Mac

OS X operating system, code-named Tiger, will be available on April 29.

The Cupertino, California-based maker of Macintosh computers and iPod digital music players has long said that Tiger would be shipped by the first half of the year.

The updated operating system – which serves as the nerve center controlling the functions of all the features of the computer – is expected to fuel interest in Apple's computers, already energized by products including the Mac Mini and the iPod digital music player. However, some consumers may delay a decision to buy until the new software is released.

Tiger, which will sell for about $129, includes new features such as Spotlight, Apple's advanced desktop search function that scours the computer's hard disk drive to find documents, e-mail, pictures and music, similar to the way Google searches the Internet.

The operating system also has Dashboard, which is a collection of Internet-enabled programs to give users instant information on airline flights, movie times, weather, stock prices and other information.

Microsoft Corp.'s next major version of its operating systems, code-named Longhorn, has been delayed a number of times and is now expected in 2006. Microsoft's Windows operating systems dominates the global market.

Apple said it will sell a "family pack" version of the software, for $199, that serves up to five computers in a single residence.

Firefox Still Drawing Internet Masses

The Firefox browser continues to draw millions of users looking for an alternative to Microsoft's Internet Explorer, with Nielsen//Netratings confirming data from other market analysts showing that the open-source browser has developed a strong following in a short time.

Nielsen reports a whopping 237 percent increase in the number of visitors to the Firefox Web site – operated by open-source developer Mozilla – in the past nine months. Some 2.6 million people visited the site during March 2005 to download the browser.

The SpreadFirefox Web site, which tracks usage of the browser, reports some 45 million downloads since the launch of Firefox 1.0, late last year. This figure makes it the number-two browser, but it is still well behind Microsoft's Internet Explorer.

Recent figures from Web analytics firm OneStat.com show that Firefox has captured 8.45 percent of global usage, while Internet Explorer has dropped to below 90 percent with a usage share of 87.28 percent, down 1.62 percent since November.

Firefox might well continue to gain traction in the consumer market, although its momentum seems to have slowed somewhat. However, breaking into the enterprise arena is another matter, primarily because of compatibility issues.

The upstart browser's popularity stems from better security features and enhanced functionality, said Yankee Group analyst Nitin Gupta. "Firefox has

some innovative features that thwart pop-up ads, adware and spam, which Explorer has not yet added," he said.

Still, he noted, Web developers have not yet embraced Firefox and there are several sites that are compatible only with Explorer, such as those run by banks.

"There has been a lot of frustration with Explorer and its ongoing security problems, said Gupta. "Microsoft is monitoring Firefox closely and is expected to add a number of the features to its next browser that Firefox currently delivers."

Forrester Research analyst Michael Goulde called Firefox the "poster child" of the open-source developer community. "It is a very visible, successful product that has become the model for other-open source projects," he said.

While acknowledging that Firefox has experienced some bugs of its own, Goulde said Mozilla was able to take advantage of the door left open by Microsoft. Microsoft now is in a defensive position in the browser market, he said, with some of Firefox's popularity attributed to a backlash against the software giant.

Developers, until now, have focused on Explorer, given its dominance, but they now are being forced to target both the Microsoft and open-source environments, said Goulde.

The Mozilla Foundation's product is not the only competitor chipping away at IE's numbers. OneStat.com's data show that Apple's Safari browser has moved up from 0.91 percent usage to 1.21 percent since November. Netscape continues to hold a usage share over 1 percent, and Opera stands at 1.09 percent.

Seagate Readies New Hard Drive Technology

Seagate Technology is developing a perpendicular recording technology for hard drives and intends to be one of the first companies to use it in its products, the company said this week.

The announcement makes Seagate the third major storage device vendor to announce plans to sell products using the technology, which is a storage method that promises to significantly boost the capacity of hard drives.

Drives store data in magnetically charged bits. In today's commercially available drives the bits lay flat on the disk surface. With perpendicular drives, the bits stand upright. Because they take up less space, more room is available on the disc. Drives using the new technology should be about the same weight, and able to record and access data at about the same speeds as conventional drives.

"We invest between 8 to 10 percent of our revenue each quarter into R&D and we have invested in perpendicular technology for many years," says Randy Lee, senior vice president of global sales at Seagate, speaking at a Tokyo news conference this week.

"We will be one of the first... to introduce this to production," he says.

Lee declines to specify the company's exact schedule, but his comments

suggest that Seagate could be releasing drives as early as the middle of 2005. This is because last December, Toshiba of Japan announced that it planned to begin selling its first hard drive using perpendicular technology in the April to June quarter.

In Toshiba's case, the recording density of the drives will be about 37 percent greater than that of the company's current drives, it says.

Earlier this month, Hitachi Global Storage Technologies said that it too was testing samples of drives using perpendicular recording.

The largest capacity external hard drive currently offered by Seagate is a 400GB model that uses a 3.5-inch disk.

Murdoch Urges Editors to Embrace Internet

Rupert Murdoch urged newspaper editors Wednesday to embrace the Internet, saying print news executives have "sat by and watched" as a new generation of digital consumers has turned away from newspapers.

The chief executive of News Corp. cited a recent report commissioned by the Carnegie Corporation, a philanthropic foundation, showing 44 percent of 18-to-34-year-olds say they use Web sites at least once a day for news.

He said newspapers must overhaul how they gather and deliver news to collect the readers and advertising revenue shifting to the Web.

"The trends are against us. Unless we awaken to these changes which are quite different than those five or six years ago, we will, as an industry, be relegated to the status of also-rans," Murdoch told the annual meeting of the American Society of Newspaper Editors.

"We've been slow to react. We've sat by and watched," he said.

News Corp. is the parent company of the New York Post. The global media company also operates a number of papers in England.

When the Web was emerging in the 1990s Murdoch expressed skepticism about its business prospects. He referred to himself and other newspaper executives as "digital migrants" who are too old to have grown up surfing the Net but now must learn to direct their business toward those who did.

"Just watch your teenage kids," he told the editors.

"The challenge for each of us in this room is to create an Internet presence that is compelling enough that users make it their home page. Just as people traditionally started their day with coffee and a newspaper, in the future I hope that the way they start their day online will be with coffee and our Web site."

Murdoch's media empire began with a single Australian newspaper business. Now headquartered in the United States, News Corp. is the parent of the 20th Century Fox movie studio, Fox television network, Fox News Channel and other cable channels.

In recent years, Murdoch has sought to expand a satellite business in China, but he voiced doubts Wednesday when asked about the business

climate there.

"There are indications that it's closing up more than opening up," he said, calling the enterprise "very hard work."

Similar efforts in India have gone much better, he said, even though the potential market is significantly smaller.

Bush: 'I Don't Want You Reading My Personal Stuff'

President Bush said on Thursday he does not send e-mail, not even to his twin daughters, because he fears "my personal stuff" would be made public.

"There has got to be a certain sense of privacy," he told the American Society of Newspaper Editors.

Bush volunteered his aversion to e-mail during a discussion on whether his administration is sufficiently responsive to requests made under the Freedom of Information Act.

Advocates of greater openness in government charge the Bush administration has used the need to guard homeland security as an excuse to keep more information secret.

Bush said the government receives about 3.5 million FOIA requests a year and that he is for open government but does not want information released that could endanger lives.

"I would hope that those who expose documents are wise about the difference between that which truly would jeopardize national security and that which should be read," he said.

Sean Moulton, a spokesman at OMB Watch, a group that tracks decisions by the White House Office of Management and Budget and other government agencies, said: "This is a government that is getting worse by the day in terms of permitting the public access to information and documents that they have paid for."

He said all administrations have been difficult on the issue "but this administration is being extremely opportunistic with homeland security concerns and using that as an excuse to shut down public access."

Bush has pressured Russian President Vladimir Putin to allow for greater freedom of the press in Russia. "We got to make sure our own press is free. I know that," he said.

But when it comes to e-mail, Bush said he avoids it because "everything is investigated in Washington" and as a result "we're losing a lot of history, not just with me, but with other presidents as well."

As a result, he does not use this form of communication to talk to his twin daughters, Jenna and Barbara.

"I don't want you reading my personal stuff," he told the editors.

"There has got to be a certain sense of privacy. You know, you're entitled to how I make decisions. And you're entitled to ask questions, which I

answer. I don't think you're entitled to be able to read my mail between my
daughters and me," he said.

=~=~=~=